batman-adv - Bug #216

received packet on bat0 with own address as source address

05/30/2015 11:49 PM - A Z

Status:	Closed	**Start date:**	05/30/2015
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	2015.2		

Description

Setup:
Nodes: 3 Batman-Nodes: A; B; C + Non-Batman-Nodes: D
Network: 1 IBSS WPA2-RSN Mesh Network with Nodes A+B+C (they see each other pairwise) + 1 LAN network with B+C+D

On A+B+C: bat0 is in bridge br-wlan, which also contains eth0.513 and an AP device (where A has no wire connected to eth0)
D is the local gateway (their are other non-batman nodes in the lan as well)
A+B+C run udhcpc (DHCP client) on br-wlan, which has the same mac as eth0.513

batman_adv: B.A.T.M.A.N. advanced 2014.4.0 (compatibility version 15) loaded
batman bridge loop avoidance enabled
distributed arp table: enabled

Problem: tcpdump shows packets looping all the time, load goes up and kernel complains as given in this issues subject (an similiar for eth0.513 instead of bat0)
When DAT is disabled - or either of B or C removed from br-wlan - looping stops and everythings works flawlessy.

B> tcpdump -n -e -i bat0 arp and host 0.0.0.0
23:03:57.209922 00:0c:f1:a6:e3:25 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0b:6b:7e:9e:75, length 28
23:03:57.209813 00:0b:6b:7e:9e:75 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0c:f1:a6:e3:25, length 28
23:03:57.211611 00:0c:f1:a6:e3:25 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.212389 00:0c:f1:a6:e3:25 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0b:6b:7e:9e:75, length 28
23:03:57.218334 00:0c:f1:a6:e3:25 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0b:6b:7e:9e:75, length 28
23:03:57.217791 00:0b:6b:7e:9e:75 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0c:f1:a6:e3:25, length 28
23:03:57.219242 00:0c:f1:a6:e3:25 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.219343 00:0c:f1:a6:e3:25 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0b:6b:7e:9e:75, length 28
23:03:57.243484 30:14:4a:7f:a7:a8 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 00:0c:f1:a6:e3:25, length 42
23:03:57.243579 30:14:4a:7f:a7:a8 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 00:0c:f1:a6:e3:25, length 42
23:03:57.243851 00:0c:f1:a6:e3:25 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0b:6b:7e:9e:75, length 28
23:03:57.394645 30:14:4a:7f:a7:a8 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 43:05:43:05:95:93, length 42
23:03:57.394808 00:0b:6b:7e:9e:75 > 30:14:4a:7f:a7:a8, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 28
23:03:57.440743 66:65:6d:01:3d:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.440824 66:65:6d:01:2c:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.440872 66:65:6d:01:0e:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.440916 66:65:6d:01:50:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.440959 66:65:6d:01:39:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441003 66:65:6d:01:44:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441048 66:65:6d:01:1b:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441092 66:65:6d:01:3b:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441136 66:65:6d:01:01:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441180 66:65:6d:01:0f:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441224 66:65:6d:01:28:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441266 66:65:6d:01:0b:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441308 66:65:6d:01:11:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42

23:03:57.441352 66:65:6d:01:02:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441397 66:65:6d:01:24:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441441 66:65:6d:01:31:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441484 66:65:6d:01:05:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441535 00:12:cf:89:98:87 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441580 66:65:6d:01:10:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441626 66:65:6d:01:4c:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441683 00:12:cf:83:76:1a > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441731 66:65:6d:01:1d:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441775 66:65:6d:01:38:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441824 66:65:6d:01:1a:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441876 66:65:6d:01:42:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441921 66:65:6d:01:37:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.441970 66:65:6d:01:3c:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442023 66:65:6d:01:14:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442072 66:65:6d:01:2e:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442121 66:65:6d:01:49:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442166 66:65:6d:01:15:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442213 66:65:6d:01:13:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442259 66:65:6d:01:3e:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442351 66:65:6d:01:08:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442411 66:65:6d:01:09:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442462 66:65:6d:01:26:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442511 66:65:6d:01:12:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442560 66:65:6d:01:04:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442609 66:65:6d:01:32:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442657 66:65:6d:01:45:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442706 66:65:6d:01:41:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442754 66:65:6d:01:4b:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442799 66:65:6d:01:21:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442850 66:65:6d:01:47:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442900 66:65:6d:01:25:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442949 66:65:6d:01:18:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.442993 66:65:6d:01:07:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443042 66:65:6d:01:17:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443090 66:65:6d:01:36:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443135 66:65:6d:01:4a:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443208 66:65:6d:01:33:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443264 66:65:6d:01:34:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443316 66:65:6d:01:43:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443365 00:12:cf:81:73:dc > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443420 66:65:6d:01:48:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443469 66:65:6d:01:22:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443518 66:65:6d:01:03:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443565 66:65:6d:01:1e:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443610 66:65:6d:01:3f:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443661 00:12:cf:89:99:e9 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443707 66:65:6d:01:19:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443756 66:65:6d:01:4f:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443801 66:65:6d:01:0a:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.443850 66:65:6d:01:46:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.455405 66:65:6d:01:16:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.455485 66:65:6d:01:2d:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.462906 66:65:6d:01:0d:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.463017 66:65:6d:01:35:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.463062 66:65:6d:01:40:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.470851 66:65:6d:01:06:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.470922 00:12:cf:83:82:70 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:57.470969 30:14:4a:7f:a7:a8 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 43:05:43:05:95:93, length 42
23:03:57.488605 30:14:4a:7f:a7:a8 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 66:65:6d:01:0d:ff, length 42
23:03:57.689356 72:88:da:ac:13:a5 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0b:6b:7e:9e:75, length 28
23:03:58.015337 66:65:6d:01:1d:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0b:6b:7e:9e:75, length 28
23:03:58.030423 00:25:90:55:2b:2a > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:58.030502 30:14:4a:7f:a7:a8 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 66:65:6d:01:1d:ff, length 42

23:03:58.030700 30:14:4a:7f:a7:a8 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 00:25:90:55:2b:2a, length 42
23:03:58.032075 00:25:90:55:2b:2a > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:58.034139 66:65:6d:01:1d:ff > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0b:6b:7e:9e:75, length 28
23:03:58.049168 30:14:4a:7f:a7:a8 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 66:65:6d:01:05:ff, length 42
23:03:58.049229 30:14:4a:7f:a7:a8 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 00:25:90:55:2b:2a, length 42
23:03:58.049276 30:14:4a:7f:a7:a8 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 66:65:6d:01:06:ff, length 42
23:03:58.162374 a8:54:b2:40:16:7f > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 60: Reply 0.0.0.0 is-at 43:05:43:05:89:9a, length 46
23:03:58.209789 00:0b:6b:7e:9e:75 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0c:f1:a6:e3:25, length 28
23:03:58.211393 00:0c:f1:a6:e3:25 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:58.218521 00:0c:f1:a6:e3:25 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0b:6b:7e:9e:75, length 28
23:03:58.251034 30:14:4a:7f:a7:a8 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 00:0c:f1:a6:e3:25, length 42
23:03:58.251451 00:0c:f1:a6:e3:25 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0b:6b:7e:9e:75, length 28
23:03:58.302383 00:25:90:d3:19:74 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 30:14:4a:7f:a7:a8, length 42
23:03:58.305078 00:25:90:d3:19:74 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0b:6b:7e:9e:75, length 28
23:03:58.309042 00:25:90:55:2b:2a > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:0b:6b:7e:9e:75, length 28
23:03:58.324016 30:14:4a:7f:a7:a8 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 56: Reply 0.0.0.0 is-at 00:25:90:d3:19:74, length 42
23:03:58.338379 00:0b:6b:7e:9e:75 > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 42: Reply 0.0.0.0 is-at 00:25:90:55:2b:2a, length 28
...

B> batctl o
[B.A.T.M.A.N. adv 2014.4.0, MainIF/MAC: mesh1/00:0b:6b:7e:9e:75 (bat0 BATMAN_IV)]
Originator last-seen (#/255) Nexthop [outgoingIF]: Potential nexthops ...
a8:54:b2:40:16:7b 0.056s (251) a8:54:b2:40:16:7b [mesh1]: 30:14:4a:7f:a7:a8 (198) a8:54:b2:40:16:7b (251)
30:14:4a:7f:a7:a8 0.880s (255) 30:14:4a:7f:a7:a8 [mesh1]: a8:54:b2:40:16:7b (188) 30:14:4a:7f:a7:a8 (255)

C> batctl o
[B.A.T.M.A.N. adv 2014.4.0, MainIF/MAC: mesh1/30:14:4a:7f:a7:a8 (bat0 BATMAN_IV)]
Originator last-seen (#/255) Nexthop [outgoingIF]: Potential nexthops ...
a8:54:b2:40:16:7b 0.632s (255) a8:54:b2:40:16:7b [mesh1]: 00:0b:6b:7e:9e:75 (188) a8:54:b2:40:16:7b (255)
00:0b:6b:7e:9e:75 0.024s (247) 00:0b:6b:7e:9e:75 [mesh1]: a8:54:b2:40:16:7b (198) 00:0b:6b:7e:9e:75 (247)

B> batctl bbt
Backbones announced for the mesh bat0 (orig 00:0b:6b:7e:9e:75, group id 0xf287)
Originator VID last seen (CRC) * 30:14:4a:7f:a7:a8 on -1 2.760s (0x0000)

C>batctl bbt
Backbones announced for the mesh bat0 (orig 30:14:4a:7f:a7:a8, group id 0xf287)
Originator VID last seen (CRC) * 00:0b:6b:7e:9e:75 on -1 8.488s (0xd240)

after DAT disabled:
B> batctl cl
Claims announced for the mesh bat0 (orig 00:0b:6b:7e:9e:75, group id 0xf287)
Client VID Originator [o] (CRC) * 66:65:6d:01:1f:ff on -1 by 30:14:4a:7f:a7:a8 [ ] (0xd240)

C> batctl cl
Claims announced for the mesh bat0 (orig 30:14:4a:7f:a7:a8, group id 0xf287)
Client VID Originator [o] (CRC) * 66:65:6d:01:1f:ff on -1 by 30:14:4a:7f:a7:a8 [x] (0xd240)

which is small because it only lists the mac of br-wlan on A (66:65:6d:01:1f:ff is br-wlan mac of A)

When DAT enabled, "batctl cl" on B is big and lists all most every client on LAN as owned by C * 66:65:6d:01:01:ff on -1 by 30:14:4a:7f:a7:a8 [ ] (0x3e58)
and some by B * 66:65:6d:01:1f:ff on -1 by 00:0b:6b:7e:9e:75 [x] (0x58d6)

I think this is a bug as packets should not loop with DAT enabled.

History

#1 - 05/30/2015 11:49 PM - A Z

kernel: Linux femap0106 3.18.11 #37 SMP Sat May 30 10:09:58 CEST 2015 ppc GNU/Linux (openwrt)

#2 - 06/01/2015 02:46 PM - Simon Wunderlich

Thanks for reporting. Yes, this certainly sounds wrong.

We've been pondering but it would be very helpful if you could provide us a little more material for debugging:

- "tcpdump -i eth1 -w /tmp/dump" for about one minute to get a wireshark dissectable dump * "grep -n . /sys/class/net/*/address" to list all used mac addresses in your systems (please run on A, B, C, D) * brctl show to list bridges

Thanks!

#3 - 06/01/2015 05:34 PM - Antonio Quartulli

I just sent a patch to the mailing list addressing a problem in DAT. We are not really confident that this is going to directly address your issue, but it would be helpful to apply it before doing any further test.

The patch is called: [PATCHv2 maint] batman-adv: avoid DAT to mess up LAN state

It should apply on batman-adv 2014.4.0

#4 - 06/01/2015 05:35 PM - Antonio Quartulli

- File 0001-batman-adv-avoid-DAT-to-mess-up-LAN-state.patch added

The patch is also attached here to make it simpler for you.

#5 - 06/04/2015 08:04 AM - A Z

Thanks for the patch, I'm giving it a try.

#6 - 06/04/2015 01:20 PM - A Z

Looks like that patch does not fix it, traces will follow up.

#7 - 06/05/2015 09:01 AM - A Z

- File femap0106-tcpdump-60s.pcap.gz added

This has just happened again, but this time with dat turned off and two more nodes B' and C' that are connected just like B and C.

D is a cisco router which uses 00:1b:0d:62:b0:00

B:
/sys/class/net/bat0/address:1:0a:21:07:4e:b8:a2
/sys/class/net/br-lan/address:1:66:65:6d:01:06:ff
/sys/class/net/br-mgnt/address:1:66:65:6d:01:06:ef
/sys/class/net/br-stavpn/address:1:66:65:6d:01:06:ff
/sys/class/net/br-wlan/address:1:66:65:6d:01:06:ff
/sys/class/net/brvlan501/address:1:66:65:6d:01:06:02
/sys/class/net/dummy0/address:1:ae:82:70:ba:66:5d
/sys/class/net/eth0.513/address:1:66:65:6d:01:06:ff

/sys/class/net/eth0.515/address:1:66:65:6d:01:06:ff
/sys/class/net/eth0/address:1:66:65:6d:01:06:ff
/sys/class/net/eth1/address:1:66:65:6d:01:06:fe
/sys/class/net/eth2/address:1:66:65:6d:01:06:fd
/sys/class/net/ftwl0_1/address:1:66:65:6d:01:06:01
/sys/class/net/ftwl0_2/address:1:66:65:6d:01:06:02
/sys/class/net/ftwl1_1/address:1:66:65:6d:01:06:11
/sys/class/net/ftwl1_2/address:1:66:65:6d:01:06:12
/sys/class/net/ftwl1_6/address:1:66:65:6d:01:06:13
/sys/class/net/lo/address:1:00:00:00:00:00:00
/sys/class/net/mesh1/address:1:66:65:6d:01:06:1f
/sys/class/net/prewl0_1/address:1:66:65:6d:01:06:01
/sys/class/net/prewl1_1/address:1:66:65:6d:01:06:11
/sys/class/net/tinctap.501/address:1:66:65:6d:01:06:ef
/sys/class/net/tinctap.514/address:1:66:65:6d:01:06:ef
/sys/class/net/tinctap/address:1:66:65:6d:01:06:ef
/sys/class/net/wl0_1/address:1:66:65:6d:01:06:01
/sys/class/net/wl0_2.4096/address:1:66:65:6d:01:06:02
/sys/class/net/wl0_2/address:1:66:65:6d:01:06:02
/sys/class/net/wl1_1.4096/address:1:66:65:6d:01:06:11
/sys/class/net/wl1_1/address:1:66:65:6d:01:06:11
/sys/class/net/wl1_2/address:1:66:65:6d:01:06:12
/sys/class/net/wl1_6/address:1:66:65:6d:01:06:13
/sys/class/net/wlan0/address:1:66:65:6d:01:06:00
/sys/class/net/wlan1/address:1:66:65:6d:01:06:10

C:
/sys/class/net/bat0/address:1:26:39:90:10:09:1b
/sys/class/net/br-lan/address:1:66:65:6d:01:40:ff
/sys/class/net/br-mgnt/address:1:66:65:6d:01:40:ef
/sys/class/net/br-stavpn/address:1:66:65:6d:01:40:ff
/sys/class/net/br-wlan/address:1:66:65:6d:01:40:ff
/sys/class/net/dummy0/address:1:72:6f:e5:83:db:42
/sys/class/net/eth0.513/address:1:66:65:6d:01:40:ff
/sys/class/net/eth0.515/address:1:66:65:6d:01:40:ff
/sys/class/net/eth0/address:1:66:65:6d:01:40:ff
/sys/class/net/eth1/address:1:66:65:6d:01:40:fe
/sys/class/net/eth2/address:1:66:65:6d:01:40:fd
/sys/class/net/lo/address:1:00:00:00:00:00:00
/sys/class/net/mesh1/address:1:66:65:6d:01:40:1f
/sys/class/net/tinctap.514/address:1:66:65:6d:01:40:ef
/sys/class/net/tinctap/address:1:66:65:6d:01:40:ef
/sys/class/net/wlan0/address:1:66:65:6d:01:40:00
/sys/class/net/wlan1/address:1:66:65:6d:01:40:10

A: down

B':
/sys/class/net/bat0/address:1:26:8a:6d:26:e0:27
/sys/class/net/br-lan/address:1:66:65:6d:01:15:ff
/sys/class/net/br-mgnt/address:1:66:65:6d:01:15:ef
/sys/class/net/br-stavpn/address:1:66:65:6d:01:15:ff
/sys/class/net/br-wlan/address:1:66:65:6d:01:15:ff
/sys/class/net/dummy0/address:1:2a:de:ca:18:12:fb
/sys/class/net/eth0.513/address:1:66:65:6d:01:15:ff
/sys/class/net/eth0.515/address:1:66:65:6d:01:15:ff
/sys/class/net/eth0/address:1:66:65:6d:01:15:ff
/sys/class/net/eth1/address:1:66:65:6d:01:15:fe
/sys/class/net/eth2/address:1:66:65:6d:01:15:fd
/sys/class/net/lo/address:1:00:00:00:00:00:00
/sys/class/net/mesh1/address:1:66:65:6d:01:15:1f
/sys/class/net/tinctap.514/address:1:66:65:6d:01:15:ef
/sys/class/net/tinctap/address:1:66:65:6d:01:15:ef
/sys/class/net/wlan0/address:1:66:65:6d:01:15:00
/sys/class/net/wlan1/address:1:66:65:6d:01:15:10

C':
/sys/class/net/bat0/address:1:4e:45:ab:ad:c9:4a
/sys/class/net/br-lan/address:1:66:65:6d:01:0d:ff
/sys/class/net/br-mgnt/address:1:66:65:6d:01:0d:ef
/sys/class/net/br-stavpn/address:1:66:65:6d:01:0d:ff
/sys/class/net/br-wlan/address:1:66:65:6d:01:0d:ff
/sys/class/net/brvlan501/address:1:66:65:6d:01:0d:01
/sys/class/net/brvlan77/address:1:66:65:6d:01:0d:02
/sys/class/net/dummy0/address:1:0e:d1:82:0f:b4:c0

/sys/class/net/eth0.513/address:1:66:65:6d:01:0d:ff
/sys/class/net/eth0.515/address:1:66:65:6d:01:0d:ff
/sys/class/net/eth0/address:1:66:65:6d:01:0d:ff
/sys/class/net/eth1/address:1:66:65:6d:01:0d:fe
/sys/class/net/eth2/address:1:66:65:6d:01:0d:fd
/sys/class/net/ftwl0_1/address:1:66:65:6d:01:0d:01
/sys/class/net/ftwl0_2/address:1:66:65:6d:01:0d:02
/sys/class/net/ftwl1_1/address:1:66:65:6d:01:0d:11
/sys/class/net/ftwl1_2/address:1:66:65:6d:01:0d:12
/sys/class/net/ftwl1_6/address:1:66:65:6d:01:0d:13
/sys/class/net/lo/address:1:00:00:00:00:00:00
/sys/class/net/mesh1/address:1:66:65:6d:01:0d:1f
/sys/class/net/prewl0_1/address:1:66:65:6d:01:0d:01
/sys/class/net/prewl1_1/address:1:66:65:6d:01:0d:11
/sys/class/net/tinctap.501/address:1:66:65:6d:01:0d:ef
/sys/class/net/tinctap.514/address:1:66:65:6d:01:0d:ef
/sys/class/net/tinctap.77/address:1:66:65:6d:01:0d:ef
/sys/class/net/tinctap/address:1:66:65:6d:01:0d:ef
/sys/class/net/wl0_1.4097/address:1:66:65:6d:01:0d:01
/sys/class/net/wl0_1/address:1:66:65:6d:01:0d:01
/sys/class/net/wl0_2.4096/address:1:66:65:6d:01:0d:02
/sys/class/net/wl0_2.4097/address:1:66:65:6d:01:0d:02
/sys/class/net/wl0_2.4098/address:1:66:65:6d:01:0d:02
/sys/class/net/wl0_2/address:1:66:65:6d:01:0d:02
/sys/class/net/wl1_1.4096/address:1:66:65:6d:01:0d:11
/sys/class/net/wl1_1.4097/address:1:66:65:6d:01:0d:11
/sys/class/net/wl1_1/address:1:66:65:6d:01:0d:11
/sys/class/net/wl1_2/address:1:66:65:6d:01:0d:12
/sys/class/net/wl1_6/address:1:66:65:6d:01:0d:13
/sys/class/net/wlan0/address:1:66:65:6d:01:0d:00
/sys/class/net/wlan1/address:1:66:65:6d:01:0d:10

B:
br-lan 7fff.66656d0106ff no eth0
eth1
eth2
br-mgnt 7fff.66656d0106ef no tinctap.514
prewl1_1
ftwl1_1
ftwl1_2
ftwl1_6
prewl0_1
ftwl0_1
ftwl0_2
br-stavpn 7fff.66656d0106ff no eth0.515
wlan0
wlan1
br-wlan 7fff.66656d0106ff no eth0.513
bat0
wl1_1
wl1_6
wl0_1
wl1_1.4096
wl1_1.4097
brvlan501 8000.66656d010602 no wl0_2.4096
tinctap.501

C:
bridge name bridge id STP enabled interfaces
br-lan 7fff.66656d0140ff no eth0
eth1
eth2
br-mgnt 7fff.66656d0140ef no tinctap.514
br-stavpn 7fff.66656d0140ff no eth0.515
br-wlan 7fff.66656d0140ff no eth0.513
bat0

B':
bridge name bridge id STP enabled interfaces
br-lan 7fff.66656d0115ff no eth0
eth1
eth2
br-mgnt 7fff.66656d0115ef no tinctap.514
br-stavpn 7fff.66656d0115ff no eth0.515
br-wlan 7fff.66656d0115ff no eth0.513

bat0

C':
bridge name bridge id STP enabled interfaces
br-lan 7fff.66656d010dff no eth0
eth1
eth2
br-mgnt 7fff.66656d010def no tinctap.514
prewl1_1
ftwl1_1
ftwl1_2
ftwl1_6
prewl0_1
ftwl0_1
ftwl0_2
br-stavpn 7fff.66656d010dff no eth0.515
wlan0
wlan1
br-wlan 7fff.66656d010dff no eth0.513
bat0
wl1_1
wl1_6
wl0_1
wl1_1.4096
wl1_1.4097
brvlan77 8000.66656d010d02 no wl0_2.4096
tinctap.77
wl0_2.4098
wl0_2.4097
brvlan501 8000.66656d010d02 no wl0_2.4099
tinctap.501

#8 - 06/05/2015 09:02 AM - A Z

The issue resolved after rebooting C

#9 - 06/05/2015 09:09 AM - A Z

batctl if shows:
mesh1: active

#10 - 06/05/2015 12:47 PM - Simon Wunderlich

Thanks for the dump.

From what I can tell so far is:

- we see many BLA requests from B/mesh1 to C/mesh1. These are sent when B thinks it does not have all the BLA claims sent by C, so it asks C to repeat it. * C repeats all claims and sends an announcement as final packet * However, we see that C sends no claims at all. It only sends an announcement to finalize the reply. * In these final announcements, the CRC is e2:5c. However we would expect it to be 00:00 if there are no claims.

It looks like the CRC got out of sync for some reason. However it also look different to the "textual" dump you reported before.

How good can you reproduce that (exact) issue? I can try to write a patch to re-compute the CRC before sending out announcements ...

#11 - 06/05/2015 12:54 PM - Simon Wunderlich

One more thing, what platform are you using? This looks like a power PC?

#12 - 06/05/2015 03:54 PM - A Z

Yes, this is powerpc. I can try to reproduce with A/B/C only and DAT enabled.

#13 - 06/11/2015 06:48 PM - Simon Wunderlich

- File 0002-batman-adv-DEBUG-track-CRC-changes.patch added

- File 0001-batman-adv-lock-crc-access-in-bridge-loop-avoidance.patch added

Please find attached two patches to debug your problem further.

The first one should fix a possible problem if multiple calls change the same CRC, creating inconsistency. The second one is a debugging patch to further track the problem.

Both are based 2014.4.0. I'd like you to first test the first one only, since adding debug can alter race condition behavior. If you still see these problems, please apply the second one and reproduce with BLA logging enabled. Please provide us with logs of the nodes involved and tcpdumps as before, then.

Thank you!

#14 - 06/22/2015 05:26 PM - Simon Wunderlich

Hey, did you get the chance to test the patch(es) yet? Thanks!

#15 - 06/24/2015 10:28 AM - A Z

No I've not yet managed to test this, but I'm looking forward to do this asap.

#16 - 07/10/2015 11:20 AM - Marek Lindner

A Z wrote:

> No I've not yet managed to test this, but I'm looking forward to do this asap.

Any chance to test the patches ?

#17 - 07/21/2015 01:52 PM - A Z

I've just received new devices to test with and new firmware with patches applied is compiling. Looking forward into testing.

#18 - 09/03/2015 09:54 AM - A Z

After applying

0001-batman-adv-avoid-DAT-to-mess-up-LAN-state.patch
0001-batman-adv-lock-crc-access-in-bridge-loop-avoidance.patch
0001-batman-adv-protect-tt_local_entry-from-concurrent-de.patch
0002-batman-adv-DEBUG-track-CRC-changes.patch

from issue #216 and #217, I've not yet seen this again. But I'm not quite sure, because there are (except from the kernel crash issue) some spurious connectivity issues seen by applications running on top of the batman mesh.

#19 - 09/03/2015 10:24 AM - Simon Wunderlich

Thanks for testing! Did you test in the same environment/with the same hardware? Did the problems usually happen within that timeframe that you tested?

#20 - 09/03/2015 11:15 AM - A Z

I've been testing for 4 days with equal hardware. Connectivity was lost about every 15min probably due to #217 for 2 days, then uptime increased to > 2days (thus no crash) and this morning crashing from #217 was back. Connectivity issues occured every 1-12h during the 2 days all devices did not crash and lasted a few minutes. Though I've not hit them while I was sitting next to the devices.

#21 - 09/04/2015 03:11 PM - Simon Wunderlich

Thank you for your test, so it seems at least this issue has been removed by the patch.

I'd suggest it for inclusion on the mailing list - may I add your "tested by" tag in the commit message?

Thank you!

#22 - 09/04/2015 03:47 PM - A Z

That's fine. Thanks alot.

#23 - 01/29/2016 10:44 AM - Simon Wunderlich

- Status changed from New to Closed

Fixed

#24 - 02/11/2017 08:47 AM - Sven Eckelmann

- Target version set to 2015.2

Files

0001-batman-adv-avoid-DAT-to-mess-up-LAN-state.patch	2.77 KB	06/01/2015	Antonio Quartulli
femap0106-tcpdump-60s.pcap.gz	2.38 MB	06/05/2015	A Z
0001-batman-adv-lock-crc-access-in-bridge-loop-avoidance.patch	5.9 KB	06/11/2015	Simon Wunderlich
0002-batman-adv-DEBUG-track-CRC-changes.patch	2.97 KB	06/11/2015	Simon Wunderlich